EMBEDDING CYCLIC LATIN SQUARES OF ORDER 2^n IN A COMPLETE SET OF ORTHOGONAL F-SQUARES*

S. J. SCHWAGER
W. T. FEDERER
Biometrics Unit, Cornell University, Ithaca, New York, 14853, U.S.A.

J. P. MANDELI
Department of Mathematical Sciences, Virginia Commonwealth University, Richmond, Virginia, 23284

Abstract: A cyclic Latin square of order 2^n, which has no orthogonal Latin square mate, is shown to have $(2^n-1)(2^n-2)$ mutually orthogonal $F(2^n;2^{n-1},2^{n-1})$-squares. This is the complete set of F-squares for the mateless Latin square. Row and column operations are used to construct this complete set of F-squares from a Hadamard matrix and 2^n-1 $OF(2^n;2^{n-1},2^{n-1})$-squares into which the Latin square is decomposed. Tables of complete sets of mutually orthogonal $F(2^n;2^{n-1},2^{n-1})$-squares are given for n = 2 and 3, i.e., for mateless Latin squares of orders 4 and 8.

AMS Subject Classification: 62K99, 62K15

Key words: F-square design, orthogonal F-squares, Hadamard matrix, Hadamard product, factorial design, Latin square.

---

* Paper Number BU-788-M in the Biometrics Unit Mimeo Series, Cornell University, Ithaca, New York, 14853.

1. Introduction

An F(2λ;λ,λ)-square with two treatments or symbols or simply an F-square is a square matrix of order 2λ in which each of two symbols appears exactly λ times in every row and column. Two F(2λ;λ,λ)-squares are orthogonal if each ordered pair of symbols appears together λ^2 times when the first F-square is superimposed on the second. A set of s F(2λ;λ,λ)-squares is (mutually) orthogonal if every pair of these s F-squares are orthogonal. Such a set is denoted by OF(2λ;λ,λ;s), and is complete if $s = (2\lambda - 1)^2$. These definitions suffice for the material presented in this paper. For more general definitions and greater detail, including comments on the practical application of F-square methods, see Hedayat and Seiden (1970) and Hedayat, Raghavarao, and Seiden (1975).

A cyclic Latin square of order 2^n, for which no orthogonal Latin square exists, can be decomposed into 2^n-1 mutually orthogonal $F(2^n;2^{n-1},2^{n-1})$-squares. If $(2^n-1)(2^n-2)$ additional mutually orthogonal F-squares can be found, the result will be a complete set, $OF(2^n;2^{n-1},2^{n-1};(2^n-1)^2)$. Row and column operations have been used to construct complete sets of orthogonal F-squares for cyclic Latin squares of order four (Mandeli, 1975), order eight (Federer, Mandeli, and Schwager, 1981a), and order 16 (Federer, Mandeli, and Schwager, 1981b). It will be shown here that these operations give a complete set of orthogonal F-squares when applied to a cyclic Latin square of order 2^n for any $n \geq 2$.

The remainder of this paper is organized as follows. Further definitions and notation are presented in Section 2. Examples are given in Section 3, where the constructions for orders 4 and 8 are discussed. The proof that row and column operations yield a complete set of orthogonal F-squares for order 2^n constitutes Section 4. Concluding remarks appear in Section 5.

2. Definitions and notation

The two symbols of an F-square will be denoted by + and - in this paper. It will be helpful to view these symbols as representing the numbers +1 and -1, respectively. Multiplication follows the usual algebraic rules, (+)(+) = (-)(-) = + and (+)(-) = (-)(+) = -. The Hadamard product, element-by-element multiplication of equally-dimensioned vectors or matrices, will be denoted by $*$, and the direct or Kronecker product of vectors and matrices by $\otimes$, e.g.,

$$([+-] \otimes [++]) * ([++] \otimes [+-]) = [++--] * [+-+-] = [+--+] \quad .$$

Hadamard products will be referred to simply as products, and the product operator Π will indicate a Hadamard product. Matrix transposition will be denoted by the superscript t. The commutativity of $*$, associativity of $*$ and $\otimes$, and other easily derived elementary properties of these operators, e.g., $(u \otimes v) * (u' \otimes v') = (u*u') \otimes (v*v')$ for all conformable u, v, u', v', will be used freely. For further background information, see Searle (1982).

Let $e[\ell]$ denote the row vector of length ℓ and $E[\ell]$ the $\ell \times \ell$ square matrix consisting entirely of +'s. For $k = 1,\cdots,n$, define the row vector of length 2^n

$$g_k \equiv e[2^{k-1}] \otimes [+-] \otimes e[2^{n-k}] \quad ,$$

and define $g_0 \equiv e[2^n]$. Under the operation $*$, vectors $g_1,\cdots,g_n$ generate a finite group H^* of 2^n members with identity element g_0. The elements of H^* will be denoted by h_i, $i = 0,1,\cdots,2^n-1$. To define these as products of the generators g_k, observe that for any i from 1 to 2^n-1, there is a unique set $I(i) \subset \{1,2,\cdots,n\}$ such that $i = \Sigma_{k\in I(i)}2^{k-1}$. As is easily seen by considering the binary expression for i, $i \neq i'$ iff (if and only if) $I(i) \neq I(i')$. For $i = 1,2,\cdots,2^n-1$, define the row vector of length 2^n

$$h_i = \Pi_{k\in I(i)}g_k \quad ,$$

and define $h_0 \equiv g_0$. The vector g_k is a generator of h_i if $k \in I(i)$. For instance, $5 = 1 + 4 = 2^{1-1} + 2^{3-1}$, so $I(5) = \{1,3\}$, $h_5 = g_1 * g_3$, and the generators of h_5 are g_1 and g_3. Note that $g_k = h_m$ when $m = 2^{k-1}$ and that $h_i * h_i = h_0$ for every i.

The rows h_i, $i = 0,1,\cdots,2^n-1$ form a symmetric Hadamard matrix of order 2^n. The rows, or by symmetry the columns, correspond to factorial model main effect and interaction contrasts. Rows $h_1 = g_1$, $h_2 = g_2$, $h_4 = g_3$, $h_8 = g_4$, $\cdots$ correspond to main effects of factors A, B, C, D, $\cdots$; rows $h_3 = g_1 * g_2$, $h_5 = g_1 * g_3$, $\cdots$ correspond to two-factor interactions AB, AC, $\cdots$; rows $h_7 = g_1 * g_2 * g_3$, $\cdots$ correspond to three-factor interactions ABC, $\cdots$; and so on. Any row h_i for which g_k is a generator represents a main effect or interaction contrast involving the k^{th} factor.

Let $H(g_{k+1}, g_{k+2}, \cdots, g_n)$ denote the subgroup of H^* generated by $g_{k+1}, \cdots, g_n$, and let $H(\phi) = \{g_0\}$. Define $H \equiv H^* - H(\phi)$ and

$$H_k \equiv \{g_k * h : h \in H(g_{k+1}, \cdots, g_n)\} \quad \text{for} \quad k = 1, \cdots, n \quad .$$

Thus $H = \bigcup_{k=1}^n H_k$, the number of elements in H_k is $\#[H_k] = 2^{n-k}$, and H_k consists of all elements of H whose lowest generator is g_k.

Three classes of square matrices derived from row vectors will appear throughout this paper. For any row vector v of length ℓ, the $\ell \times \ell$ row matrix $R(v)$ corresponding to v is the standard matrix product of $e[\ell]^t$ and v,

$$R(v) \equiv e[\ell]^t v \quad ,$$

and the $\ell \times \ell$ column matrix $C(v)$ corresponding to v is the transpose of $R(v)$,

$$C(v) \equiv R(v)^t = v^t e[\ell] \quad .$$

Let the rotation by k places of $v = (v_1 \cdots v_\ell)$ be denoted by

$$k \circ v \equiv (v_{\ell-k+1}\ v_{\ell-k+2} \cdots v_\ell\ v_1\ v_2 \cdots v_{\ell-k}) \quad ,$$

and define the $\ell \times \ell$ F matrix $F(v)$ corresponding to v as the circulant matrix (see Searle (1979)) whose ℓ rows are v, $1 \circ v$, $2 \circ v$, $\cdots$, and $(\ell - 1) \circ v$. This F matrix is an F-square whenever ℓ is even and v has equal numbers of +'s and -'s.

Let k denote a nonnegative integer. A row vector or row is symmetric of order 2^k or $SO(2^k)$ with root w if it consists of 2^k copies of a row vector w concatenated, i.e., it is of the form $(w,w,\cdots,w)$ with the arbitrary row vector w appearing 2^k times. A row vector is antisymmetric of order 2^k or $ASO(2^k)$ with root w if it is the concatenation of 2^k row vectors that are alternating copies of a row vector w and its (element-by-element) negative, i.e., it is of the form $(w,-w,w,-w,\cdots,w,-w)$ with w and -w appearing 2^{k-1} times each. A matrix is symmetric of order 2^k or $SO(2^k)$ if each of its rows is $SO(2^k)$, and a matrix is antisymmetric of order 2^k or $ASO(2^k)$ if each of its rows is $ASO(2^k)$. An example that will prove useful in Section 3 is the row vector g_k, which is both $ASO(2^k)$ and $SO(2^{k-1})$. More general definitions of symmetric and antisymmetric row vectors and matrices could be given, but these are sufficient for the work presented here.

A row operation on the F matrix $F(v)$ is element-by-element multiplication of $F(v)$ and a row matrix $R(v')$, yielding $F(v) * R(v')$. A column operation on $F(v)$ is element-by-element multiplication of $F(v)$ and a column matrix $C(v')$, yielding $F(v) * C(v')$. If a row (column) operation produces an F-square, this square is a row (column) operation F-square.

3. The embedding for orders 4 and 8

For order 4, consider the cyclic Latin square and the Hadamard matrix

$$F(1\ 2\ 3\ 4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{bmatrix} = \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \end{bmatrix} = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_1 * g_2 \end{bmatrix} .$$

The Latin square decomposes into the three orthogonal F-squares

$$F(h_1) = \begin{bmatrix} + & + & - & - \\ - & + & + & - \\ - & - & + & + \\ + & - & - & + \end{bmatrix}, \quad F(h_2) = \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}, \quad \text{and} \quad F(h_3) = \begin{bmatrix} + & - & - & + \\ + & + & - & - \\ - & + & + & - \\ - & - & + & + \end{bmatrix} .$$

There are nine possible row operations $F(h_i)*R(h_j)$ with $i,j = 1,2,3$, and nine corresponding column operations $F(h_i)*C(h_j)$. Some of these $(F(h_2)*R(h_1)$, $F(h_2)*R(h_3)$, $F(h_2)*C(h_1)$, $F(h_2)*C(h_3))$ yield unique F-squares orthogonal to $F(h_1)$, $F(h_2)$, $F(h_3)$, and all other row and column operation F-squares; some $(F(h_1)*R(h_2) = F(h_3)*C(h_2)$, $F(h_3)*R(h_2) = F(h_1)*C(h_2))$ yield F-squares that appear twice and have the same orthogonality property; and the rest do not yield F-squares. For instance,

$$F(h_2)*R(h_1) = \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix} * \begin{bmatrix} + & + & - & - \\ + & + & - & - \\ + & + & - & - \\ + & + & - & - \end{bmatrix} = \begin{bmatrix} + & - & - & + \\ - & + & + & - \\ + & - & - & + \\ - & + & + & - \end{bmatrix} ;$$

$$F(h_1)*R(h_2) = \begin{bmatrix} + & - & - & + \\ - & - & + & + \\ - & + & + & - \\ + & + & - & - \end{bmatrix} ; \qquad F(h_1)*R(h_1) = \begin{bmatrix} + & + & + & + \\ - & + & - & + \\ - & - & - & - \\ + & - & + & - \end{bmatrix} .$$

Table 1 summarizes these results, using notation defined in the next two paragraphs, where the case of order 8 is discussed.

For order 8, consider the cyclic Latin square $F(1\ 2 \cdots 8)$ and the Hadamard matrix given in Figure 1. It is easily checked that $H_1 = \{h_1, h_3, h_5, h_7\}$, $H_2 = \{h_2, h_6\}$, and $H_3 = \{h_4\}$. The Latin square decomposes into the seven orthogonal F-squares $F(h_i)$, $i = 1,\cdots,7$. There are 49 possible row operations $F(h_i)*R(h_j)$ with $i,j = 1,\cdots,7$, and the same number of column operations. When these are examined, four cases arise. (A) Some yield unique F-squares orthogonal to the original seven F-squares and to every new F-square produced. (B) Some yield F-squares appearing twice, once from a row operation and once from a column operation, that are orthogonal to all original and new F-squares. (C) Certain column (row) operations yield F-squares that are unique and orthogonal to all original and column (row) operation F-squares, but are not orthogonal to some row (column) operation F-squares. (D) Some do not yield F-squares.

Table 2 lists the F-squares obtained from row and column operations; A, B, C, and - indicate that both row and column operations produce F-squares of the types described in (A), (B), (C), and (D), respectively. Performing all row operations and then all column operations shows that the table gives 14 + 6 + 8 + 14 = 42 mutually orthogonal F-squares. This embeds the original Latin square in a complete set of orthogonal F-squares. In the next section, it is proved that an embedding of this type is accomplished by the row and column procedure for a cyclic Latin square of order 2^n for any $n \geq 2$.

Table 1

Six mutually orthogonal F-squares of order 4 obtained by row and column operations

Original F-square $F(h_i)$, $i = 1,2,3$	Row and column operations $R(h_j)$ and $C(h_j)$, $j = 1,2,3$: 1	2	3
1	-	B	-
2	A	-	A
3	-	B	-

Symbols A, B, and - are explained in text

Figure 1

Cyclic Latin square F(1 2 ··· 8) and Hadamard matrix of order 8

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 8 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{bmatrix} ; \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \\ + & + & - & - & - & - & + & + \\ + & - & + & - & + & - & + & - \\ + & - & + & - & - & + & - & + \\ + & - & - & + & + & - & - & + \\ + & - & - & + & - & + & + & - \end{bmatrix} = \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{bmatrix} = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_1 * g_2 \\ g_3 \\ g_1 * g_3 \\ g_2 * g_3 \\ g_1 * g_2 * g_3 \end{bmatrix}$$

Table 2

Forty-two mutually orthogonal F-squares of order 8 obtained by row and column operations

Original F-square $F(h_i)$, $i = 1,\cdots,7$	Row and column operations $R(h_j)$ and $C(h_j)$, $j = 1,\cdots,7$: 1	2	3	4	5	6	7
1	-	C	-	B	-	C	-
2	A	-	A	B	A	-	A
3	-	C	-	B	-	C	-
4	A	A	A	-	A	A	A
5	-	C	-	B	-	C	-
6	A	-	A	B	A	-	A
7	-	C	-	B	-	C	-

Symbols A, B, C, and - are explained in text

4. The embedding for order 2^n

Some useful symmetry properties of rows and their (Hadamard) products and rotations will now be given. Routine proofs will be omitted.

Lemma 4.1. Any $ASO(2^k)$ *row with* $k \geq 1$ *is* $SO(2^{k-1})$. *Any* $SO(2^k)$ *row with* $k \geq 1$ *is* $SO(2^{k-1})$. *These statements also hold for matrices.*

Lemma 4.2. The (Hadamard) product of two $ASO(2^k)$ *rows is a* $SO(2^k)$ *row. The product of two* $SO(2^k)$ *rows is a* $SO(2^k)$ *row. The product of an* $ASO(2^k)$ *row and a* $SO(2^k)$ *row is an* $ASO(2^k)$ *row. These statements also hold for matrices.*

Lemma 4.3. The rotation by ℓ *places of an* $ASO(2^k)$ *row is* $ASO(2^k)$ *for any* ℓ. *The rotation by* ℓ *places of a* $SO(2^k)$ *row is* $SO(2^k)$ *for any* ℓ.

All rows, columns, and square matrices from here to the end of this section are of order 2^n unless there is an explicit indication to the contrary.

Lemma 4.4. The row g_k *is* $ASO(2^k)$ *for* $k = 1,\cdots,n$.

Lemma 4.5. If $h_i \in H_k$, *then* h_i, $F(h_i)$, *and* $R(h_i)$ *are* $ASO(2^k)$.

Proof. The row h_i is a product $g_k{*}h$, where h is the product of some subset of $\{g_{k+1},\cdots,g_n\}$, possibly the null product g_0. Since each of $g_{k+1},\cdots,g_n$ and g_0 is $SO(2^k)$ by Lemmas 4.4 and 4.1, the product h is $SO(2^k)$ and $h_i = g_k{*}h$ is $ASO(2^k)$ by Lemmas 4.4 and 4.2. Lemma 4.3 completes the proof for $F(h_i)$.

Lemma 4.6. Let h_i *be* $ASO(2^k)$ *with root* w. *Then* $F(h_i) = E[2^{k-1}] \otimes F(w,-w)$ *and* $R(h_i) = E[2^{k-1}] \otimes R(w,-w)$, *where* $F(w,-w)$ *and* $R(w,-w)$ *are the square, order*

2^{n-k+1} *F matrix and row matrix corresponding to the row vector* $(w,-w)$ *of length* 2^{n-k+1}.

Lemma 4.7. If $F(h_i)$ *is* $ASO(2^k)$, *then its transpose* $F(h_i)^t$ *is* $ASO(2^k)$. *If* $F(h_i)$ *is* $SO(2^k)$, *then* $F(h_i)^t$ *is* $SO(2^k)$.

The first major step after these preliminaries is to find the conditions under which performing a row or column operation on $F(h_i)$ produces an F-square.

Theorem 4.1. Take $h_i \in H_k$ *and* $h_j \in H_{k'}$, *where* $1 \le k, k' \le n$. *The products* $F(h_i)*R(h_j)$ *and* $F(h_i)*C(h_j)$ *are F-squares iff* $k' \neq k$.

Proof. Assume $k' \neq k$. (i) If $k' > k$, then $F(h_i)$ is $ASO(2^k)$ by Lemma 4.5 and $R(h_j)$ is $SO(2^k)$ by Lemmas 4.5 and 4.1, so $P \equiv F(h_i)*R(h_j)$ is $ASO(2^k)$ by Lemma 4.2. Each row of P therefore has equal numbers of +'s and -'s, 2^{n-1} of each. Each column of P is either a duplicate of the corresponding column of the F-square $F(h_i)$ or its negative, hence has 2^{n-1} +'s and 2^{n-1} -'s. Thus P is an F-square. (ii) If $k' < k$, then $F(h_i)$ is $SO(2^{k'})$ and $R(h_j)$ is $ASO(2^{k'})$, so P is $ASO(2^{k'})$, and the reasoning just used shows that P is an F-square.

Assume now that $k' = k$. It will be established that the number of +'s varies from row to row of P, which suffices to show that P is not an F-square. (i) If $k' = k = 1$, then $h_j = g_1*h_{j'}$ for some $h_{j'}$ that is $SO(2^1)$ as shown in the proof of Lemma 4.5, and g_1 is $ASO(2^1)$ from Lemma 4.4. The matrix $P = F(h_i)*R(g_1)*R(h_{j'})$ is a product of two $ASO(2^1)$ and one $SO(2^1)$ matrices, so it is $SO(2^1)$, making its left half and right half identical. Note also that the left halves of $F(h_i)$ and $F(h_i)*R(g_1)$ are identical. Compare the left halves of any two adjacent rows, e.g., the first and the second, of $F(h_i)$. The difference d between the numbers of +'s in these two left halves will now be shown to be an odd integer.

Let $\#(x,x')$ denote the number of positions in the row's left half at which (a) the upper row of $F(h_i)$ being considered contains x and (b) the row below it in $F(h_i)$ contains x'. Let $\#(x,x';x'')$ denote the number of positions in the row's left half at which (a) and (b) hold and (c) the row $h_{j'}$ contains x''. The rotation of the lower row of $F(h_i)$ by one more place than the row above it changes by ± 1 the number of +'s in the row's left half. Thus, in moving from the upper row of $F(h_i)$ to the row below it, the number of positions in the row's left half where + changes to - differs by ± 1 from the number of positions where - changes to +:

$$\#(+,-) = \#(-,+) \pm 1 = \#(+,-;+) + \#(+,-;-) = \#(-,+;+) + \#(-,+;-) \pm 1 \ . \quad (1)$$

The number of +'s in the left half of the upper row of P is $\#(+,+;+) + \#(+,-;+) + \#(-,+;-) + \#(-,-;-)$, and the number of +'s in the left half of the following row of P is $\#(+,+;+) + \#(-,+;+) + \#(+,-;-) + \#(-,-;-)$, so their difference is $d = \#(-,+;+) + \#(+,-;-) - \#(+,-;+) - \#(-,+;-)$. Solving equation (1) for $\#(+,-;+)$ and substituting into the formula for d gives $d = 2\#(+,-;-) \pm 1$, which must be an odd integer. Thus the number of +'s differs from one row of P to the next row, by two times an odd number, which establishes that P is not an F-square.

(ii) If $k' = k > 1$, then $F(h_i) = E[2^{k-1}] \otimes F(w,-w)$ and $R(h_j) = E[2^{k-1}] \otimes R(w',-w')$ by Lemma 4.6, where w and w' are the roots of h_i and h_j, respectively. Therefore, $P = E[2^{k-1}] \otimes Q$ where $Q \equiv F(w,-w)*R(w',-w')$. The rows $(w,-w)$ and $(w',-w')$ of length 2^{n-k+1} are $ASO(2^1)$, so the analysis just presented for the case $k' = k = 1$, with P replaced by Q and n by $n - k + 1$, shows that the number of +'s differs from one row to the next of Q, and thus of P.

For column operations, note that $F(h_i)*C(h_j)$ is an F-square iff its transpose $F(h_i)^t*R(h_j)$ is one. Using Lemma 4.7, the analysis for row operations applies to this transpose with only minor modifications, concluding the proof of the theorem.

The next two theorems establish the orthogonality of all F-squares resulting from row (column) operations and the duplication of certain F-squares that are formed once from a row operation and once from a column operation.

Theorem 4.2. When all possible $(2^n-1)^2$ row operations $F(h_i)*R(h_j)$ with $i,j = 1,\cdots,2^n-1$ are performed, $\frac{2}{3}(2^n-1)(2^n-2)$ of these produce F-squares, which are mutually orthogonal and orthogonal to every original F-square $F(h_i)$. The same result holds for column operations.

Proof. The number of row operation F-squares is

$$\sum_{k=1}^{n} \#[H_k]\#[H-H_k] = \sum_{k=1}^{n} 2^{n-k}(2^n-1-2^{n-k}) = \frac{2}{3}(2^n-1)(2^n-2) .$$

Two F-squares are orthogonal iff their (Hadamard) product contains equal numbers of +'s and -'s. Consider the product of any pair of distinct row operation F-squares,

$$S \equiv [F(h_i)*R(h_j)]*[F(h_{i'})*R(h_{j'})] = F(h_i*h_{i'})*R(h_j*h_{j'}) \quad .$$

If $i = i'$, then $F(h_i*h_{i'}) = F(h_0)$ consists entirely of +'s and $h_{j''} \equiv h_j*h_{j'} \neq h_0$, so $S = R(h_{j''})$, which has equal numbers of +'s and -'s. If $i \neq i'$, then $h_{i''} \equiv h_i*h_{i'} \neq h_0$, so $F(h_{i''})$ has equal numbers of +'s and -'s in each column. This property is preserved under Hadamard multiplication by $R(h)$ for an arbitrary row vector h, and again S has equal numbers of +'s and -'s. This establishes mutual orthogonality. The orthogonality of $F(h_i)*R(h_j)$ to any $F(h_{i'})$ follows from the same reasoning with j replacing j''. Column operations are immediate using transposition.

Theorem 4.3. Let $i' = i+2^{n-1}$ for $i = 0,1,\cdots,2^{n-1}-1$ and $i' = i-2^{n-1}$ for $i = 2^{n-1},\cdots,2^n-1$, and let $m = 2^{n-1}$. Then $F(h_i)*R(h_m) = F(h_{i'})*C(h_m)$ for each i, and this product is an F-square for $i \neq 0,m$.

Proof. It is easy to demonstrate that $F(h_{i'}) = F(h_i)*F(h_m)$ for any i and that $F(h_m)*C(h_m) = R(h_m)$. Therefore,

$$F(h_i)*R(h_m) = F(h_i)*F(h_m)*C(h_m) = F(h_{i'})*C(h_m) \quad .$$

By Theorem 4.1, this is an F-square if $i \neq 0,m$. For $i = 0,m$, either h_i or $h_{i'}$ equals h_0, so the product is not an F-square.

The next theorem specifies which column operation F-squares are orthogonal to every row operation F-square, and vice versa. It will provide enough orthogonal column operation F-squares in addition to the set of all row operation F-squares to result in a complete set.

Theorem 4.4. A column operation F-square $F(h_i)*C(h_j)$ is orthogonal to every row operation F-square iff $h_i \in H_k$ and $h_j \in \bigcup_{\ell=1}^{k-1} H_\ell$ for some $k = 2,3,\cdots,n$. There are $\frac{1}{3}(2^n-1)(2^n-2)$ column operation F-squares of this type. A column operation F-square $F(h_i)*C(h_j)$ is not orthogonal to some row operation F-square iff $h_i \in H_k$ and $h_j \in \bigcup_{\ell=k+1}^{n} H_\ell$ for some $k = 1,\cdots,n-1$. The statements remain true if the roles of row and column operations are interchanged.

Proof. Choose any i, j, i', j' such that for some k, k': $h_i \in H_k$, $h_j \in \bigcup_{\ell=1}^{k-1} H_\ell$, $h_{i'} \in H_{k'}$, and $h_{j'} \in H-H_{k'}$. Define $h_{i''} \equiv h_i * h_{i'}$ and consider the (Hadamard) product

$$S \equiv [F(h_i)*C(h_j)] * [F(h_{i'})*R(h_{j'})] = F(h_{i''})*C(h_j)*R(h_{j'}) \quad .$$

If $k' \geq k$, then $h_{i''} \in H_{k''}$ for some $k'' \geq k$, and $h_j \in H-H_{k''}$, so $F(h_{i''})*C(h_j)$ is an F-square by Theorem 4.1. Hadamard multiplication by $R(h_{j'})$ preserves the equal numbers of +'s and -'s in each column, so S contains equal numbers of +'s and -'s. If $k' < k$, then $h_{i''} \in H_{k'}$ and $F(h_{i''})*R(h_{j'})$ is an F-square by Theorem 4.1. Hadamard multiplication by $C(h_j)$ preserves the equal numbers of +'s and -'s in each row, so again S contains equal numbers of +'s and -'s. This implies orthogonality of $F(h_i)*C(h_j)$ and $F(h_{i'})*R(h_{j'})$.

The number of F-squares $F(h_i)*C(h_j)$ with $h_i \in H_k$, $h_j \in \cup_{\ell=1}^{k-1} H_\ell$ for some $k = 2,\cdots,n$ is

$$\sum_{k=2}^{n} \#[H_k] \left(\sum_{\ell=1}^{k-1} \#[H_\ell]\right) = \sum_{k=2}^{n} 2^{n-k} \sum_{\ell=1}^{k-1} 2^{n-\ell} = \tfrac{1}{3}(2^n-1)(2^n-2) .$$

These have already been shown to be orthogonal to the original F-squares $F(h_i)$ and to each other in Theorem 4.2. Combining them with the 2^n-1 original F-squares and the set of all row operation F-squares gives a complete set $OF(2^n;\ 2^{n-1},2^{n-1};(2^n-1)^2)$. This set contains the maximal number of orthogonal F-squares possible (Hedayat, Raghavarao, and Seiden (1975)), so all remaining column operation F-squares must lack orthogonality to some member(s) of the set. Any such F-square $F(h_i)*C(h_j)$ must have $h_i \in H_k$, $h_j \in \cup_{\ell=k+1}^{n} H_\ell$ for some $k = 1,\cdots,n-1$ by Theorem 4.1, and must lack orthogonality to some row operation F-square by Theorem 4.2.

Combining Theorems 4.1 to 4.4 yields the main result:

<u>Theorem 4.5. A cyclic Latin square of order</u> 2^n, $n \geq 2$, <u>which has no orthogonal Latin square, can be embedded in a complete set of orthogonal</u> $F(2^n;\ 2^{n-1},2^{n-1})$<u>-squares with two treatments or symbols. Decompose the cyclic Latin square into the</u> 2^n-1 <u>orthogonal F-squares</u> $F(h_i)$, <u>form all</u> $(2^n-1)^2$ <u>row operation squares</u> $F(h_i)*R(h_j)$, $i,j=1,\cdots,2^n-1$, <u>and then form all</u> $(2^n-1)^2$ <u>column operation squares</u> $F(h_i)*C(h_j)$. <u>The row operation squares consist of:</u>

(i) $\frac{2}{3}(2^n-1)(2^n-2)$ <u>F-squares that are orthogonal to each other and to the original F-squares; and</u>

(ii) $\frac{1}{3}(2^{2n}-1)$ squares that are not F-squares.

The column operation squares consist of:

(iii) $\frac{1}{3}(2^n-1)(2^n-2)$ F-squares that are orthogonal to each other, to the original F-squares, and to the row operation F-squares from (i);

(iv) 2^n-2 F-squares that are duplicates of F-squares from (i);

(v) $\frac{1}{3}(2^n-2)(2^n-4)$ F-squares that are orthogonal to each other, to the original F-squares, and to the column operation F-squares from (iii) and (iv), but are not orthogonal to the set of row operation F-squares from (i); and

(vi) $\frac{1}{3}(2^{2n}-1)$ squares that are not F-squares.

The 2^n-1 original F-squares and the $(2^n-1)(2^n-2)$ F-squares of (i) and (iii) provide a complete set of orthogonal $F(2^n;2^{n-1},2^{n-1})$-squares with two symbols, in which the cyclic Latin square is embedded. The structure of the sets of squares in (i)-(vi) is specified in Theorems 4.1 to 4.4. These results all remain true if the roles of row operations and column operations are reversed. A different complete set of orthogonal F-squares is produced by this interchange for $n > 2$.

5. Concluding remarks

Row and column operation squares were generated and the orthogonality relations of the F-squares among them, to the original F-squares and to each other, were calculated with computer assistance. Checking by hand even a single 8×8 or 16×16 matrix of +'s and -'s to determine whether it is an F-square, or a single pair of F-squares to determine whether they are orthogonal, is quite laborious and susceptible to error. Using a computer for arithmetic involving large collections of 8×8 and 16×16 matrices was an attractive alternative to hand calculation, especially since the formulation of the approach to the general 2^n case was based on the patterns that emerged from the special cases of orders 8 and 16. Computer programs for finding the row and column operation F-squares and checking orthogonality were written in the APL language by the first author, and are available on request. They took advantage of the extremely efficient handling of 0-1 matrices, whose storage required only one bit per entry, by using 0 and 1 to replace the symbols - and +.

The question of whether cyclic Latin squares of orders other than 2^n can be embedded in a complete set of orthogonal F-squares is a natural one. The only results to date are negative, involving the cyclic Latin squares of orders $2\lambda = 12, 20$, and 24. Each of these squares was decomposed into $2\lambda-1$ orthogonal $F(2\lambda;\lambda,\lambda)$-squares, which are F matrices corresponding to rows h_1 to $h_{2\lambda-1}$ of an order 2λ Hadamard matrix (Hedayat and Wallis, 1978, pp. 1222-1223) whose first row is $h_0 \equiv e[2\lambda]$. In each case, when the row and column operations were performed on the F-squares $F(h_1)$ to $F(h_{2\lambda-1})$, no F-squares were obtained. The nature of the geometries suggests that the row and column procedure will never embed the cyclic Latin square in a complete set of $OF(2\lambda;\lambda,\lambda)$-squares. This situation may extend to cyclic Latin squares of order $4t \neq 2^n$.

References

Federer, W. T., J. P. Mandeli and S. J. Schwager (1981a). On a complete set of orthogonal F-squares of order 8 with a mateless Latin square. No. BU-753-M, Mimeo Series, Biometrics Unit, Cornell University, Ithaca, New York.

Federer, W. T., J. P. Mandeli and S. J. Schwager (1981b). On embedding mateless Latin squares of orders 12 and 16 in a complete set of orthogonal F-squares. No. BU-759-M, Mimeo Series, Biometrics Unit, Cornell University, Ithaca, New York.

Hedayat, A., D. Raghavarao and E. Seiden (1975). Further contributions to the theory of F-squares designs. Ann. Statist. 3, 712-716.

Hedayat, A. and E. Seiden (1970). F-square and orthogonal F-squares design: A generalization of Latin square and orthogonal Latin squares design. Ann. Math. Statist. 41, 2035-2044.

Hedayat, A. and W. D. Wallis (1978). Hadamard matrices and their applications. Ann. Statist. 6, 1184-1238.

Mandeli, J. P. (1975). Complete sets of orthogonal F-squares. M.S. Thesis, Cornell University, Ithaca, New York.

Searle, S. R. (1979). On inverting circulant matrices. Linear Algebra and Appl. 25, 77-89.

Searle, S. R. (1982). Matrix Algebra Useful for Statistics. Wiley, New York.